HOODSWEENEY

The latest internet threat - Cryptolocker

Protect yourself from vicious malware

Investing in professional IT systems protection might seem like unnecessary expenditure but it can be nothing in comparison to the cost of losing all your data, warns Hood Sweeney.

Imagine fronting up to your business on Monday morning, appointment books full, the phone ringing and you cannot access your files or the billing data, client records, and referrals because they are encrypted and illegible.

That's a scenario that has faced many business hit by the wave of malware including the vicious Cryptolocker, which has been doing the rounds over the past few months.

Hood Sweeney IT director Graham Wadsley says any business that cannot afford to have 24 hours' IT down time or cannot afford to lose data must be prepared to invest in a range of measures to protect itself from Internet bugs and other disaster.

"Victims might be sent an email that advises them to click on a link and the link will take them to a website that will initiate file encryption. They could get a web page that says that their files are being held to ransom because of the encryption. Or they may not even get that – they might just find that their files have been encrypted and they've got a problem… There are businesses that have had hundreds of megabytes of data encrypted," Graham says.

It is therefore important to get professional help to maximise protection against Internet threats and disaster – particularly because malware such as the Cryptolocker continues to evolve, he says.

Hood Sweeney's IT team employs a range of measures for clients, ensuring that protection strategies are regularly monitored and maintained.

"We supply, install and maintain systems for maximising protection whether it is anti-virus, firewall devices or anti-spam solutions – we manage all of that on behalf of our clients, including educating their people about not clicking on things they don't understand. The people element is the tough one," Graham says.

T 1300 764 200 **F** 08 8232 1968
info@hoodsweeney.com.au
www.hoodsweeney.com.au

HOODSWEENEY

Graham says any business that cannot afford to be without their IT systems for more than 24 hours, should maximise protection by:

- Installing anti-virus software on all equipment
- Using hosted anti-spam capability
- Using edge protection (installing a device at the point where the internet connection is made to inspect the traffic to assist in blocking attacks such as a Cryptolocker attack)
- Educating people about how to manage IT risks.

"You have got to maintain quality back-ups that are reliable because if you do get caught you need a way of getting your information back and in the absence of a backup, you have potentially lost everything," Graham says.

Increasingly businesses are using external back-up and disaster recovery services as they are ever more reliant on their technology which is potentially vulnerable to a range of natural disasters, accidents and crime.

It is very time consuming to build an IT environment from scratch after a disaster. The impact on business (from technology failure) is becoming greater.

"We used to talk about taking 3-4 days to recover an (IT) environment as being acceptable but we now know that the Recovery Time Objective for business is getting closer to 24 hours. That is hard to achieve unless you have a hosted solution where you back up somewhere else with a disaster recovery option, so if you have a disaster, the host starts up your environment for you," Graham says.

Yet it is important to obtain professional advice about the best option for backing up data, particularly given privacy considerations associated with housing sensitive customer or patient data offshore.

Constant monitoring is also critical because businesses are often unaware that there is something wrong with their system until too late and clients have gone elsewhere.

"I think the Cryptolocker message is that you've just got to spend the money to protect yourself because if you get caught, it can be devastating - especially if you don't have reliable back ups," Graham says.

The Technology Services team at Hood Sweeney specialises in reliable, cost-effective and scalable solutions for information and communications, including:

- outsourced CIO role
- strategic planning and consulting
- management of information technology projects
- analysing and selecting systems
- designing technology architecture
- planning for disaster recovery and business continuity
- cloud solutions
- mobile devices and communications solutions
- supporting your network and infrastructure
- help desk and user support (managed services agreements)
- procuring hardware and software.

Keith Rutherford
Senior Director
Technology Services
keith.rutherford@hoodsweeney.com.au

Graham Wadsley
Director
Technology Services
graham.wadsley@hoodsweeney.com.au

TL-Cryptolocker180815FA